

CLAIMS

What is claimed is:

1. A method for an authentication process within a data
5 processing system, the method comprising:

receiving at a single sign-on (SSO) agent an initial
authentication request for a user;

authenticating the user at the SSO agent for the
initial authentication request;

10 retrieving by the SSO agent an attribute certificate
associated with the user; and

authenticating the user for subsequent
authentication requests via the SSO agent using
authentication data within the attribute certificate.

15 2. The method of claim 1 further comprising:

retrieving a private key associated with the user;

extracting encrypted authentication data from the
attribute certificate, wherein the encrypted
20 authentication data was generated by encrypting
authentication data with a public key associated with the
user; and

decrypting the encrypted authentication data locally
using the private key associated with the user in order
25 to extract authentication data for a protected resource.

3. The method of claim 1 further comprising:

forwarding the authentication data to a protected
resource.

4. The method of claim 3 wherein the protected resource is a legacy application.

5. The method of claim 3 further comprising:

5 approving the user for access to the protected
resource based on the authentication data.

6. The method of claim 3, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

15

7. The method of claim 1 wherein the authentication data comprises a user identity and a password.

8. The method of claim 1 wherein the attribute
20 certificate is formatted according to an X.509 standard.

9. A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

5 a signature;

a holder name;

an attribute containing encrypted authentication data that was generated by encrypting multiple sets of authentication data for protected resources with a public
10 key associated with a user by a network single sign-on (SSO) agent.

10. The data structure of claim 9 wherein the protected resource is a legacy application.

15

4304280

means for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

10

means for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

15

means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

25

means for forwarding the authentication data to a protected resource.

30

14. The apparatus of claim 13 wherein the protected resource is a legacy application.

19. A computer program product in a computer-readable medium for use in a data processing system for an authentication process, the computer program product comprising:

- 5 instructions for receiving at a single sign-on (SSO) agent an initial authentication request for a user;
- instructions for authenticating the user at the SSO agent for the initial authentication request;
- instructions for retrieving by the SSO agent an
- 10 attribute certificate associated with the user; and
- instructions for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

15

20. The computer program product of claim 19 further comprising:

- instructions for retrieving a private key associated with the user;
- 20 instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and
- 25 instructions for decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

FOIA b 7 - D

21. The computer program product of claim 19 further comprising:

instructions for forwarding the authentication data to a protected resource.

5

22. The computer program product of claim 21 wherein the protected resource is a legacy application.

23. The computer program product of claim 21 further comprising:

instructions for approving the user for access to the protected resource based on the authentication data.

10

24. The computer program product of claim 21, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the computer program product further comprising:

15

instructions for parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

20

25. The computer program product of claim 19 wherein the authentication data comprises a user identity and a password.

25

26. The computer program product of claim 19 wherein the attribute certificate is formatted according to an X.509 standard.

30